AO 91 (Rev. 11/11) Criminal Complaint

SEALED

UNITED STATES DISTRICT COURT

FILED

JUN 27 2019

CLERK, U.S. DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA
BY DEPUTY CLERK

for the

Eastern District of California

United States of America
v.

ARMANDO CHRISTOPHER TABAREZ

Defendant(s)

Case No. 2:19-MJ-0102 CKD

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of June 1, 2019 in the county of Sacramento in the Eastern District of California, the defendant(s) violated:

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1)	Possession with intent to distribute methamphetamine, cocaine, and heroin,

This criminal complaint is based on these facts:

(see attachment)

☒ Continued on the attached sheet.

Complainant's signature

DAVID SIEBER
FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 6/27/2019

Judge's signature

City and state: Sacramento CA

Carolyn K. Delaney, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT OF FBI SPECIAL AGENT DAVID SIEBER

I, Federal Bureau of Investigation Special Agent David Sieber, being duly sworn, hereby depose and state:

CRIMINAL COMPLAINT FOR ARREST WARRANT AND SEARCH WARRANTS

1. This Affidavit is submitted in support of an arrest warrant and a criminal complaint charging **Armando Christopher Tabarez** with:

   COUNT ONE: Possession with intent to distribute methamphetamine, cocaine, heroin, a violation of 21 U.S.C. § 841(a)(1).

2. This Affidavit is also submitted in support of search warrants for the following items:

   ITEMS TO BE SEARCHED
   Telephone 1 – Dark Grey iPhone, Model A1634 (Described in Attachment A-1)
   Telephone 2 – Rose Gold iPhone, Model A1633 (Described in Attachment A-2)
   Telephone 3 – Blue "LG", Model LMQ610MA (Described in Attachment A-3)

BACKGROUND AND EXPERTISE

3. I am a special agent with the FBI. I entered on duty at the FBI Academy in Quantico, Virginia on October 6, 2002. I am currently assigned to the FBI's Sacramento Division, Violent Crime Safe Streets Task Force. I have been assigned to this squad since 2011.

4. During the course of my employment as an FBI special agent, I have participated in numerous criminal and national security investigations. I have also participated in numerous investigations involving the use of federal and state search warrants to collect evidence, including controlled substances, the seizure of narcotics-related records, and other types of evidence that document the activities of criminal organizations in both the manufacturing and distribution of controlled substances and weapons. To successfully conduct these investigations, I have utilized a variety of investigative techniques and resources including physical and electronic surveillance, various types of infiltration (including undercover agents, informants, and confidential human sources), pen register and trap and trace devices, GPS and telephone tracking devices, trash covers, mail covers, pole cameras, stationary video recording vehicles, audio and audio/video recording devices.

5. I am an "investigative or law enforcement officer" of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am an officer of the United States empowered by law to conduct criminal investigations and make arrests for offenses enumerated in 18 U.S.C. § 2516.

6. Because this affidavit is submitted for the limited purpose of establishing probable cause for the requested complaint, search and arrest warrant, I have not included each and every fact known to me about this case. Rather, I have set forth only the facts that I believe are necessary to support probable cause.

7. This affidavit is based upon my own personal knowledge and upon the knowledge of other law enforcement officers involved in this investigation. Where I describe statements made by other people (including other special agents and law enforcement officers), the statements are described in sum, substance, and relevant part. Similarly, where I describe information contained in reports and other documents or records in this affidavit, this information is described in sum, substance, and relevant part.

STATEMENT OF PROBABLE CAUSE

8. The FBI's Sacramento Division Safe Street Task Force (SSTF) has been investigating the drug trafficking activities of **Armando Christopher Tabarez,** hereinafter **Tabarez,** since April 29, 2019. **Tabarez'** criminal history includes the following felony convictions:

    - September 20, 1994 – Conspiracy to possess with intent to distribute methamphetamine in violation of 21 USC § 846 and § 841(A)(1), for which he was sentenced to 264 months in federal prison.

    - September 10, 2015 - Threaten with intent to terrorize in violation of California Penal Code Section 422, and Felon in possession of a firearm in violation of California Penal Code Section 29800(A)(1).

    - September 15, 2015 – Federal supervised release violation (18 USC § 3606), Arrest and return of a federal probationer, for which he was sentenced to 18 months in federal prison.

    - **Tabarez** is currently on active California state parole.

9. On May 28, 2019, FBI Confidential Human Source, hereinafter CHS-1[1], reported that Sacramento-area resident Arnold Butler, aka "Day Day," had recently been arrested in Cheyenne, Wyoming for drug trafficking offenses. CHS-1 believed that Butler's activities were connected to a drug trafficking organization run by **Armando Tabarez**. CHS-1 had previously reported that **Tabarez** served time in federal prison for drug trafficking offenses. CHS-1 added that **Tabarez** was currently coordinating kilogram-level drug shipments to Sacramento from Southern California. CHS-1 also admitted that he/she had previously couriered and stored controlled substances for **Tabarez**.

10. Open source analysis confirmed that Butler was stopped by the Wyoming Highway Patrol on Interstate 80, east of Cheyenne, on May 14, 2019. Coordination with the U.S. Attorney's Office for the District of Wyoming (DOW) revealed that Butler was operating a tow truck and hauling a car while driving through Cheyenne. The truck was stopped and the car mounted on the tow truck was searched revealing more than fifty pounds of controlled substances including methamphetamine, cocaine, heroin and fentanyl. Butler was arrested and ultimately charged by the DOW for violations of the controlled substances act.

---

[1] CHS-1 is a recently developed source who is cooperating with the federal government to reduce his/her perceived exposure to criminal prosecution stemming from an unrelated FBI narcotics investigation. In January 2009, CHS-1 received a felony conviction for causing harm to an elder in violation of California Penal Code Section 368(B)(1), for which he/she was sentenced to two years in California state prison. In November 2015, CHS-1 received a misdemeanor conviction for spousal battery in violation of California Penal Code Section 243(E)(1). CHS-1 has not received remuneration for his/her assistance. Prior to May 31, 2009, CHS-1's reporting was considered reliable based on the FBI's independent corroboration of much of his/her reporting.

However, on May 30, 2019, **Armando Tabarez**, described in more detail in this affidavit, asked CHS-1 to pick up methamphetamine for him in Southern California. The FBI instructed CHS-1 not to fulfill this task for **Tabarez**. On May 31, 2019, CHS-1 learned that **Tabarez** was sending someone else to pick up the methamphetamine on June 1st or 2nd, 2019; however, CHS-1 was uncertain exactly who was being sent. CHS-1 has reported that on May 31, 2019, at about 10:00 p.m., **Tabarez** contacted CHS-1 and asked him/her to "make a play" (sell drugs for him). CHS-1 reported to the FBI that he/she declined and then at about 11:45 p.m., after CHS-1 had fallen asleep, **Tabarez** sent another message to CHS-1 confirming that the "trap was set" (drugs were present at the stash house). CHS-1 reports that he/she did not read this message until the following day, on June 1, 2019, at approximately 12:50 p.m.

CHS-1 provided handling agents with misleading information as to the status of the methamphetamine delivery at 1 Shoal Court and timing of **Tabarez'** message regarding the "trap being set." Later in the evening on June 1, 2019, CHS-1 was interviewed. During this interview and several follow-up interviews, CHS-1 explained that he/she provided misleading information to handling agents because he was afraid handling agents would be angry for his/her failure to provide timely reporting on the unfolding events late in the evening on May 31, 2019, after he/she fell asleep, and on June 1, 2019, for failing to notify agents of the message he/she received from **Tabarez** late in the evening of May 31, 2019.

11. Subsequent telephone analysis conducted by the DEA's Wyoming and Sacramento Field offices identified a series of text communications between Butler and other unidentified persons. Based on my training experience and other experienced narcotics investigators, I believe these text communications related to a drug transaction. Specifically, on May 10, 2019, Butler exchanged text communications with telephone number 916-236-7001, which is believed to be used by **Tabarez**.[2] The text communications revealed what I believe was a drug delivery/exchange, arranged by **Tabarez**, between Butler and an unidentified third person in Southern California.

12. CHS-1 reported that **Tabarez** was currently storing a variety of controlled substances at a "trap house" located at 1 Shoal Court, #53, Sacramento, California, hereinafter "the trap house." CHS-1 believed that an unidentified parolee rented the trap house on behalf of **Tabarez** and that **Tabarez** visited the trap house several times each day. CHS-1 reported that **Tabarez** conducted narcotics sales transactions across the street from the trap house at the Greenhaven Plaza shopping center.

13. On May 29, 2019, based on the aforementioned reporting from CHS-1, the FBI initiated surveillance at **Tabarez'** suspected residences, including the trap house. **Tabarez** was not observed during surveillance on that day; however, an African-American male, later identified as Tio Sessoms, was observed entering and exiting near the trap house. A list of tenants associated with the Westlake Apartments at 1 Shoal Court identified Sessoms as the tenant of record for the trap house. Law enforcement database checks confirmed that Sessoms was on active parole in the state of California and was the responsible party for Sacramento Municipal Utilities District (SMUD) service at the trap house.

14. On May 30, 2019, **Tabarez** contacted CHS-1 and asked him/her to clear out the trunk of his/her car and drive to Los Angeles to pick up the "windows" for him. CHS-1 explained that "windows" was code for methamphetamine. FBI handlers instructed CHS-1 not to carry out this task for **Tabarez**. **Tabarez** became enraged when CHS-1 declined but ultimately said he would find someone else to pick up the methamphetamine.

15. At the behest of the FBI, CHS-1 executed a ruse by asking **Tabarez** to inform him/her when his methamphetamine arrived in Sacramento so that he/she (CHS-1) could supply one of his/her downstream customers. **Tabarez** agreed to let CHS-1 know when the methamphetamine arrived.

---

[2] On May 28, 2019, **Tabarez** checked in with his California Parole Agent using telephone number 916-236-7001. This number is listed on **Tabarez'** California parole face sheet as a cell phone contact number.

16. On May 31, 2019, **Tabarez** showed up unannounced at CHS-1's residence and asked again if he/she would pick up methamphetamine for him. Once again, CHS-1 declined **Tabarez'** request.

17. On May 31, 2019, at about 1:00 p.m., a concealed video transmitter/recorder was deployed at the trap house. The camera's view of the front door of the trap house was unobstructed. At approximately 1:31 p.m., **Tabarez** was video recorded "keying" (placing a key into the lock) of the front door of the trap house and entering with a bag in his hands. At about 2:41 p.m., **Tabarez** was captured departing the trap house and locking the door behind him. At approximately 9:27 p.m., **Tabarez** was captured "keying" (unlocking) the front door and entering the trap house while carrying a plastic grocery bag and then departing at approximately 9:43 p.m.

18. Later in the evening, on May 31, 2019, at approximately 11:28 p.m., a heavy-set male wearing a dark-colored ball cap, short pants and a white t-shirt was video recorded keying the door and entering the trap house. The male made several trips from the parking lot into the trap house while carrying cardboard boxes and at one point a bag. At about 11:34 p.m. the unidentified male locked the door and departed the trap house.

19. On the morning of June 1, 2019, Agents reviewed surveillance video from the evening of May 31, 2019. Based on physical characteristics and mannerisms, investigators initially suspected CHS-1 was the unidentified male that delivered the boxes. However, based on additional video analysis and investigation, John Terry Lopez, one of **Tabarez'** relatives, was identified as the unidentified male.

20. On June 1, 2019, at approximately 7:47 a.m., **Tabarez** was video recorded keying the door and then entering the front door of the trap house. At about 8:00 a.m., **Tabarez** was video recorded departing the trap, locking the door behind and carrying a "Home Depot" cardboard box. At about 8:12 a.m., **Tabarez** was video recorded "keying" and entering the trap house through the front door. At approximately 8:30 a.m., an unidentified female, later identified as Sherri Thornton, knocked on the front door of the trap house and was let in by an occupant inside the trap house that was not visible on the video recorder. At this point, surveillance video had only identified **Tabarez** enter the trap house. At approximately 8:53 a.m., **Tabarez** was captured exiting the trap house. At approximately 8:57 a.m., **Tabarez** let himself back into the trap house. At approximately 9:19 a.m., **Tabarez** and the unidentified female (Thornton) were captured departing from the trap house.

21. In addition to the stationary video surveillance at the trap house, FBI Special Agent (SA) Tim Damm and Sacramento County Sheriff's Department Task Force Officer (TFO)

Adam Tedford conducted surveillance on **Tabarez** as he departed the trap house at 9:19 a.m. SA Damm observed **Tabarez** depart as the driver and sole occupant of a silver Toyota Sienna minivan bearing California license plate number 7NOX844.

22. TFO Tedford observed **Tabarez** turn northbound on Florin road to Riverside Blvd. **Tabarez** stopped at the red light and turned eastbound on Riverside Blvd. **Tabarez** was travelling at approximately 55MPH in an area with a posted speed limit of 40 MPH. **Tabarez'** California Department of Motor Vehicles records indicated he had a suspended/revoked California driver's license.

23. **Tabarez** continued passing a second posted 40 MPH speed limit sign while travelling at approximately 55MPH. TFO Tedford attempted to conduct a vehicle stop on **Tabarez** by activating emergency lights and a siren on his unmarked FBI vehicle. **Tabarez** continued, failing to yield to the emergency lights and siren. **Tabarez** turned north on to Riverside Blvd cutting off oncoming traffic, still refusing to stop, despite the fact that **Tabarez** could be seen looking back at TFO Tedford's vehicle through his driver's side mirror. **Tabarez** continued to speed until coming to an abrupt stop in the middle of the roadway at Riverside Blvd and Rio Vaile Court in Sacramento.

24. **Tabarez** exited the Toyota minivan and took off running northbound across the roadway and up a Sacramento River levee. TFO Tedford came to a stop with his lights and siren still operating and giving verbal commands. **Tabarez** looked back and ignored the verbal commands to stop running and get on the ground. TFO Tedford and SA Damm engaged in a short foot pursuit with **Tabarez**. **Tabarez** had a grocery bag in his right hand and a cellular phone with a black case in his left hand. **Tabarez** ran down the back side of the levee and jumped into the Sacramento River.

25. TFO Tedford and SA Damm remained on the river bank and did not enter the water. **Tabarez** reached into the grocery bag and pulled out two large clear zip lock bags and began dumping a clear crystal-like substance, believed to be methamphetamine, into the Sacramento River. SA Damm and TFO Tedford continued to give verbal commands ordering **Tabarez** to stop destroying evidence. **Tabarez** ignored the commands and continued to destroy the suspected methamphetamine. Once the bags were empty, **Tabarez** attempted to swim across the river and then turned around and swam back to the shore. Based on the fact that blood was pouring from **Tabarez'** head, emergency medical services were requested. At about 9:31 a.m. **Tabarez** complied with commands, crawled out of the river and was taken into custody. Investigators located **Telephone 1 – Grey iPhone, Model A1634 (Described in Attachment A-1)** on the river bank close to where Tabarez had been seen in the water. Investigators located **Telephone 2 – Rose Gold iPhone, Model A1633 (Described in Attachment A-2)** in shallow water near the same

area where **Telephone 1** was found. **Telephone 2** had a black case that held **Tabarez's** driver's license.

26. Based on CHS-1's reporting and the video recordings, a search warrant for the trap house was prepared and applied for in Sacramento County. The Honorable Shelley Anne Chang swore in California Highway Patrol TFO Mike Perry and then at approximately 9:47 a.m., signed the search warrant ordering a search of the trap house.

27. At approximately 10:33 a.m., prior to executing the search warrant at the trap house, TFO Tedford and FBI SA Dave Sieber conducted a search of **Tabarez'** Toyota minivan before it was towed. During the search, $15,390.00 in U.S. currency was seized in a lunch box cooler inside the passenger compartment. In addition, court documents bearing **Tabarez'** name and **Telephone 3 – Blue "LG", Model LMQ610MA (Described in Attachment A-3**) were located inside the cooler.

28. The concealed video recorder continued to run without interruption at the trap house. No persons were observed entering or exiting the trap house after **Tabarez** departed at 9:19 a.m. At approximately 11:15 a.m., members of the SSTF initiated knock and notice procedures and executed the search warrant at the trap house.

29. The search of the trap house resulted in the seizure of the following controlled substances. All drug weights include packaging:

    - 40 Ziploc bags of Nartec positive methamphetamine - 43,846 grams
    - 5 brick-shaped packages containing Nartec positive heroin – 4357.7 grams
    - 6 heat-sealed packages containing Nartec positive cocaine – 8236 grams
    - 1 Ziploc style bag containing an unidentified hard white substance – 692.1 grams
    - 1 clear bag of green leafy substance (suspected marijuana) – 498.7 grams
    - 2 brick-shaped objects in Ziploc bags (suspected cocaine) – 1595.7 grams
    - 1 Ziploc bag containing suspected heroin – 339.1 grams
    - 2 Ziploc bags containing suspected methamphetamine – 830.3 grams
    - 7 bags of suspected marijuana – 2302 grams

30. In addition to the seizure of the aforementioned controlled substances, the following drug sales and packaging indicia were photographed at the trap: Re-sealable plastic containers, boxes of Ziploc baggies, scales, commercial boxes of heat-seal bags, a heat sealer, U.S. Postal Service boxes and "Inositol" (common cocaine cutting agent).

31. At approximately 1:00 p.m., the search was completed and all evidence was seized. At approximately 1:11 p.m., a copy of the signed search warrant was left on the kitchen table along with an FD-597 FBI Receipt for Property.

SEARCH OF DIGITAL INFORMATION

32. Your affiant is aware that drug and firearms traffickers, including **Tabarez,** use computers, smart phones, and other electronic media to conduct their trade. As described above and in Attachment B, your affiant submits that computers, smart phones, and possibly other storage media may contain evidence of **Tabarez'** ongoing criminal conduct and there is probable cause to s those items for the reasons stated below. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

33. For example, based on my knowledge, training, and experience, your affiant is aware that a powered-on computer maintains volatile data. Volatile data can be defined as active information temporarily reflecting a computer's current state including registers, caches, physical and virtual memory, network connections, network shares, running processes, disks (floppy, tape and/or CD-ROM), and printing activity. Collected volatile data may contain such information as opened files, connections to other computers, passwords used for encryption, the presence of anti-forensic tools, or the presence of programs loaded in

memory that would otherwise go unnoticed. Volatile data and its corresponding evidentiary value is lost when a computer is powered-off and unplugged.

34. Based on my knowledge, training, and experience, your affiant knows that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little to no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

35. Also, again based on your affiant's training and experience, wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

36. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, the purpose of their use, who used them, and when.

37. Thus, the forensic analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment.

38. In cases of this sort, laptop computers and/or smartphones are also used as instrumentalities of the crime to commit offenses involving interstate drug sales and movement of drug proceeds. Devices such as modems and routers can contain information about dates, frequency, and computer(s) used to access the Internet. The laptop or smart phone may also have fingerprints on them indicating the user of the computer and its components.

39. Similarly, files related to the purchasing and selling of controlled substances, as well as, the movement of currency found on computers and other digital communications devices are usually obtained from the Internet or the cellular data networks using application software which often leaves files, logs or file remnants which would tend to show the identity of the person engaging in the conduct as well as the method of location or creation of the data, search terms used, exchange, transfer, distribution, possession or origin of the files. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary internet directory or "cache". The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed internet pages or if a user takes steps to delete them. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

40. "User attribution" evidence can also be found on a computer and is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time. Your affiant knows from training and experience that digital software or hardware exists that allows persons to share digital access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of

these items can reveal information about the authorized or unauthorized use of internet connection at the residence.

41. Searching the phone(s) for the evidence described in the attachment may require a range of data analysis techniques. For example, information regarding user attribution or internet use is located in various operating system log files that are not easily located or reviewed. In addition, a person engaged in criminal activity will attempt to conceal evidence of the activity by "hiding" files or giving them deceptive names. As explained above, because the warrant calls for records of how a computer has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this location (the computer) for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

42. Based upon knowledge, training and experience, your affiant knows that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

43. The nature of evidence: As noted above, not all evidence takes the form of documents and files that can be easily viewed on-site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. Also, because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

44. The volume of evidence and time required for an examination: Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file

names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Reviewing information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

45. Technical requirements: Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off- site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

46. Variety of forms of electronic media: Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

47. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to, computer-assisted scans of the entire medium that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

48. Based on the above information, I believe that there is probable cause to believe that **Armando Christopher Tabarez** violated 21 U.S.C. § 841(a)(1), possession with the intent to distribute methamphetamine; 21 U.S.C. § 841(a)(1), possession with the intent to distribute cocaine and 21 U.S.C. § 841(a)(1), possession with the intent to distribute heroin. I hereby request that this court issue an arrest warrant for **Tabarez**. Additionally, I believe there is probable cause to believe that the identified items to be searched may

contain evidence of **Tabarez'** ongoing criminal conduct. I hereby request that this court issue search warrants for the following items:

ITEMS TO BE SEARCHED

Telephone 1 – Grey iPhone, Model A1634 (Described in Attachment A-1)
Telephone 2 - Rose Gold iPhone, Model A1633 (Described in Attachment A-2)
Telephone 3 – Blue "LG", Model LMQ610MA (Described in Attachment A-3)

REQUEST FOR SEALING

49. I further request that the Court order that all papers in support of this application, including the Affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize law enforcement efforts to enforce the warrant. Also, premature disclosure may pose a risk to executing law enforcement. It is respectfully requested that this Court issue an order

sealing, until further order the Court or court of competent jurisdiction, all papers submitted in support of this Affidavit, the accompanying search warrant, and application.

I swear, under the penalty of perjury, that the foregoing information is true and correct to the best of my knowledge, information, and belief.

DAVID SIEBER
FBI Special Agent

Sworn and Subscribed to me
on June 27, 2019

Hon. Carolyn K. Delaney
United States Magistrate Judge

Approved as to form:

/s/VINCENZA RABENN
VINCENZA RABENN
Assistant United States Attorney

ATTACHMENT A-1

The property to be searched is a **Grey iPhone, Model A1634**, hereinafter "Telephone 1." The Device is currently in the possession of the Federal Bureau of Investigation.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT A-2

The property to be searched is a **Rose Gold iPhone, Model A1633**, hereinafter "Telephone 2." The Device is currently in the possession of the Federal Bureau of Investigation.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT A-3

The property to be searched is a **Blue "LG", Model LMQ610MA**, hereinafter "Telephone 3." The Device is currently in the possession of the Federal Bureau of Investigation.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records on the Device described in Attachment A-1, A-2 and A-3 that relate to violations of 21 U.S.C. §§ 841(a) and 846, Conspiracy to Distribute a Controlled Substance, and that involve **Armando TABAREZ**. These records include:

1. Any and all names, words, telephone numbers, email addresses, time/date information, messages or other electronic data in the memory of the mobile telephone or on a server and associated with the mobile telephone, including:
    i. Incoming call history;
    ii. Outgoing call history;
    iii. Missed call history;
    iv. Outgoing text messages;
    v. Incoming text messages;
    vi. Draft text messages;
    vii. Telephone book;
    viii. Data screen or file identifying the telephone number associated with the mobile telephone searched;
    ix. Data screen, file, or writing containing serial numbers or other information to identify the mobile telephone searched;
    x. Voicemail;
    xi. User-entered messages (such as to-do lists); and
    xii. Stored media such as photographs or video.
2. Any passwords used to access the electronic data described above.
3. Evidence of user attribution showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted.
4. Any and all locations, addresses, GPS coordinates, names, time/date information, or other electronic data related to addresses and driving directions.
5. Data and information related to stored applications and/or websites used to communicate with associates and co-conspirators.
6. Lists of customers and related identifying information.

7. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions.

8. Any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information).

9. All bank records, checks, credit card bills, account information, and other financial records.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.